SKRIPSI

IMPLEMENTASI KEAMANAN JARINGAN *WIRELESS* LAN MENGGUNAKAN PROTOKOL EAP-TLS DI PT. TANJUNGENIM LESTARI *PULP AND PAPER*

Oleh:

Ahmad Fathoni

NIM: 20552010009

PROGRAM STUDI ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SUMATERA SELATAN

2024

SKRIPSI

IMPLEMENTASI KEAMANAN JARINGAN *WIRELESS* LAN MENGGUNAKAN PROTOKOL EAP-TLS DI PT. TANJUNGENIM LESTARI *PULP AND PAPER*

Laporan ini disusun untuk memenuhi salah satu persyaratan untuk mendapat Gelar Sarjana S1

Oleh:

Ahmad Fathoni

NIM: 20552010009

PROGRAM STUDI ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SUMATERA SELATAN

2024

HALAMAN PENGESAHAN SKRIPSI

Nama : Ahmad Fathoni

NIM : 20552010009

Program Studi : Ilmu Komputer

Judul Skripsi : Implementasi Keamanan Jaringan *Wireless* LAN Menggunakan Protokol EAP-TLS Di PT. Tanjungenim Lestari *Pulp and Paper*

Telah dipertahankan dihadapan dewan penguji skripsi Program Studi Ilmu Komputer Fakultas Ilmu Komputer Universitas Sumatera Selatan dan dinyatakan LULUS pada hari Sabtu, 20 Juli 2024 di Universitas Sumatera Selatan.

Palembang, 20 Juli 2024

Ketua Penguji

Usep Teisnajaya, S.Kom., M.Kom
NIDN. 0221028101

Penguji I

Ubaidillah, S.Kom., M.Kom
NIDN. 0227127402

Penguji II

Ruswa Dwipa, S.Kom., M.M
NIDN. 0215067403

Mengetahui,

Dekan

Dr. M. Taufik Roseno, M.Kom
NIDN. 0023037705

Kepala Program Studi

Serly Oktarina, S.Kom., M.Kom
NIDN. 0215109003

ABSTRAK

Jaringan *Wireless* LAN saat ini menjadi kebutuhan infrastruktur jaringan komputer yang penting di perusahaan. Keamanan jaringan *wireless* LAN menjadi sangat penting mengingat pertukaran data yang sensitif dan informasi perusahaan yang berjalan melalui jaringan tersebut. Adanya lubang keamanan pada jaringan *wireless* LAN dapat dimanfaatkan oleh siapa pun untuk melakukan tindakan ilegal seperti penyadapan. Protokol EAP-TLS (*Extensible Authentication Protocol-Transport Layer Security*) sebagai pilihan yang sangat efektif dan aman untuk mengamankan akses ke jaringan *wireless* LAN. EAP-TLS merupakan metode autentikasi EAP berdasarkan sertifikat. EAP-TLS menggunakan sertifikat kunci publik untuk autentikasi dari komputer klien ke *server* dan *server* ke komputer klien. Pada metode enkripsi menggunakan WPA/WPA2 enterprise yang mana metode ini menggunakan *server* radius dan kresidensial individu untuk setiap pengguna atau perangkat. Pada penelitian mengunakan *Network Development Life Cycle* (NDLC) dengan tahapan Analisa, Desain, Simulasi, Implementasi, Monitoring, dan Management. *Server* Radius menggunakan *Windows Server* 2008 R2 dengan dukungan *role* ADCS (*Active Directory Certificate Service*) dan NPS (*Network Policy Server*). Pembuatan radius *client* untuk *Access point* menggunakan port 1812 dengan mendaftarkan *IP addess* dan *shared secret* pada *server* Radius. C*lient* menggunakan sertifikat digital yang diinstal untuk dapat akses dan mendapatkan layanan di jaringan lokal.

Kata kunci: Jaringan nirkabel, EAP-TLS, *Enterprise*, Enkripsi, *Server* radius

ABSTRACT

Wireless LAN networks are currently an important computer network infrastructure requirement in companies. Wireless LAN network security is very important considering the exchange of sensitive data and company information that runs through the network. The existence of security holes in wireless LAN networks can be exploited by anyone to carry out illegal actions such as wiretapping. The EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) protocol is a very effective and safe choice for securing access to wireless LAN networks. EAP-TLS is an EAP authentication method based on certificates. EAP-TLS uses public key certificates for authentication from client computers to servers and servers to client computers. The encryption method uses WPA/WPA2 enterprise, which uses a radius server and individual credentials for each user or device. The study used the Network Development Life Cycle (NDLC) with the stages of Analysis, Design, Simulation, Implementation, Monitoring, and Management. The Radius server uses Windows Server 2008 R2 with support for ADCS (Active Directory Certificate Service) and NPS (Network Policy Server) roles. Creating a radius client for Access point using port 1812 by registering the IP address and shared secret on the Radius server. The client uses the installed digital certificate to be able to access and get services on the local network.

Keywords: Wireless network, EAP-TLS, Enterprise, Encryption, Radius server